

UNITED STATES DISTRICT COURT

for the
District of New HampshireIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

15 Craven Terrace, Derry, New Hampshire

Case No. 1:21-mj-74-01-AJ

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Please see attachment A.

located in the _____ District of New Hampshire, there is now concealed (identify the person or describe the property to be seized):

Please see attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1030(a)(2)(C)	Accessing a protected computer without authorization to obtain information
18 U.S.C. § 1343	Wire fraud

The application is based on these facts:

Please see attached affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


/s/ Damien A. Colon

Applicant's signature

S.A. Damien A. Colon, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 _____ telephone (specify reliable electronic means).

Date: 03/17/2021

Judge's signature

City and state: Concord, New Hampshire

Hon. Andrea K. Johnstone, U.S. Magistrate Judge

Printed name and title



UNITED STATES DISTRICT COURT)
)
DISTRICT OF NEW HAMPSHIRE)

AFFIDAVIT

I, Damien A. Colon, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since approximately May 2015. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to computer network exploitation, unauthorized access to computer networks, economic espionage, theft of trade secrets, and wire fraud. I have participated in the execution of multiple search warrants.

2. This affidavit is made in support of an application for a warrant to search the single family residence located at 15 Craven Terrace, Derry, New Hampshire, further described in Attachment A ("**Subject Premises**"), for evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030 and 1343 (the "**Subject Offenses**"), further described in Attachment B.

3. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence,

instrumentalities, and fruits of violations of Title 18, United States Code, Sections 1030 and 1343, are located in the **Subject Premises**.

I. SUMMARY

4. As detailed below, an international company located in the Northern District of Illinois (“Company A”) was the victim of a cyber attack in which a then-unidentified cyber actor (the “UCA”) gained unauthorized access to Company A’s computer network beginning on or about September 28, 2020. After obtaining access to Company A’s computer network, the UCA made changes to Company A’s active directory,¹ navigated to servers that hosted applications used to develop and store Company A software source code, elevated privileges, and exfiltrated software source code. According to Company A, the exfiltrated source code was integrated into Company A communication devices and used to unlock features on its communication devices.

5. Based on Company A network logs, agent interviews of Company A employees, and records provided by multiple internet service providers, the UCA appears to be ANDREW MAHN, a former Company A employee, who resides at the **Subject Premises**.

II. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH

a. The Spear-phishing Attack on Company A

6. According to Company A, during the initial phase of the cyber attack,

¹ According to techtarget.com, and based on my training and experience, the main service offered by active directory is domain services. Domain services verify access when a user signs into a device or attempts to connect to a server over a network. Active Directory Domain Services controls which users have access to each resource, like a file or application.

the UCA sent spear-phishing emails to thirty-one unique Company A employee email addresses in four waves from August 7, 2020 through September 29, 2020.

7. More specifically, the spear-phishing emails sent from noreply@comm-[Company A abbreviation].com (Subject Account 4)² ostensibly prompted recipients to log into their Company A accounts and provided a hyperlink that led to a fake Company A login page hosted at Subject Account 1 (comm-[Company A abbreviation].com).

8. In my review of search warrant results for Subject Account 4, I observed numerous spear-phishing emails, including this example:³

eTime User,
There is a task awaiting your approval in ADP Payroll (eTime). Please click
here
hxxps://comm-[Company A abbreviation]
[.]com/oamprod/employee_login_new/request_id2486818476358574275/ to log
into eTime and view the message. Your prompt attention is appreciated.

Message Subject: Approvals Pending
Notification Date: 8/7/2020
Regards,
[Company A] Payroll Team.

9. According to a report from Company A's Enterprise Information Security Team ("EIS Team"), the fake login page linked to in the email above

² On October 30, 2020, the Honorable Jeffrey Cummings, U.S. Magistrate Judge for the United States District Court for the Northern District of Illinois, issued a warrant (20 M 571) to NameCheap, Inc. for the search of a domain and corresponding email addresses associated with UCA activity, namely comm-[Company A abbreviation].com ("Subject Account 1"), mail-comm-[Company A abbreviation].com ("Subject Account 2"), sds@comm-[Company A abbreviation].com ("Subject Account 3"), noreply@comm-[Company A abbreviation].com ("Subject Account 4"), and harper@comm-[Company A abbreviation].com ("Subject Account 5").

³ In excerpts throughout this affidavit, "hxxps" has been substituted for "https" to prevent accidental loading by a web browser.

contained both "User ID" and "Password" fields. Additionally, Company A kept internal network logs (provided to the FBI by the EIS Team) which documented Company A employees' receipt of the spear-phishing emails, the UCA's attempts to log into Company A's network using spear-phished credentials, and Company A employees who entered their data into the fake landing page. According to these logs, at least five of the spear-phishing email recipients input their Company A employee credentials into the fake login page.

10. According to Company A, after harvesting Company A employee login credentials via the fake login page, the UCA contacted at least one of the spear-phishing email recipients via text messages using +12242768645 ("Subject Phone 1"). (Company A provided the FBI with screenshots of these text messages, as discussed further below, which I have also reviewed.) According to Google records, Subject Phone 1 was a Google Voice number associated with the Google Account ID 86326613646 (Subject Account 6), which was registered using Subject Account 5 (harper@comm-[Company A abbreviation].com).⁴ According to Company A, and as confirmed by my review of the messages, the text messages were intended to socially engineer⁵ a Company A employee ("Individual B") into providing a multi-factor authentication code, which when combined with Individual B's username and password, would allow the UCA to gain access to Company A's computer network.

⁴ Subject Account 6 was also included in the search warrants issued on October 30, 2020.

⁵ According to csoonline.com, and based on my training and experience, social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems, or data. For example, a social engineer might call an employee and pose as an information technology support employee within their organization to trick the employee into divulging his/her password.

According to Company A, the UCA obtained Individual B's multi-factor authentication code on or about September 28, 2020. Company A obtained screenshots of some of these messages from at least one of the employees who received these spear-phishing emails and related text messages. The following messages, contained in the EIS Report, are examples of text messages sent from Subject Phone 1 to a Company A employee:

Reminder: [Company A] Okta Periodic Security Verification: Verify this phone for your [Company A] Okta access. Reply YES if this phone is still assigned to [Company A employee]. Reply NO to de-link this phone from [Company A employee].

Okta Message: We're having issues verifying you. If you're unable to verify your phone now, we'll automatically try again later (Code 410).

No response received. Please reply to this conversation with the 6-8 digit code sent to your mobile device. We'll try again in a moment, or later if the process cannot be completed at this time.

11. According to Subject Account 4 email search warrant results, Individual B previously received emails from Subject Account 4 that appeared to prepare him for receipt of UCA text messages relating to Company A network authentication. For example, on September 2, 2020, Individual B received the following email:

Okta Single-Sign-On (SSO) Verification Notice

All Okta users will receive within the next 14 days a text message from the Okta verification service. This text message will originate from an Illinois area code for US-based employees. This text message confirms your two-factor device is still in use and is assigned to the user it was originally registered to. Response to this text message is required or your device will be unregistered and you will be unable to access [Company A] VPN services without re-registering via your directory supervisor's account. When the text message arrives, follow the prompts. You will be sent a 4-8-digit code. This code must be sent back to the verification service via text message to confirm your account...

12. According to Company A network logs detailing the UCA's activity on its network ("EIS Logs"), after gaining full access to Individual B's Company A account, the UCA added phone numbers to Individual B's user profile, which permitted the UCA to have persistent access to the Individual B's account through phone numbers controlled by the UCA. As a result of these profile changes, two-factor authentication codes were then sent to UCA-held phone numbers rather than to the Company A employee.

13. According to Company A, the UCA's familiarity with Company A's network infrastructure and applications was apparent based on the content of the spear-phishing emails and the content of the fake login page. More specifically, the spear-phishing emails sent from Subject Account 4 referenced and included the logo for a communication application developed and utilized by Company A. Further, the subject lines of the spear-phishing emails referenced legitimate communication application workgroups within Company A. Lastly, according to Company A, the fake login page resembled a legitimate login page last utilized by Company A in approximately 2018 (which, as discussed below, is when MAHN last worked for Company A).

14. According to Company A, the UCA's familiarity with Company A's computer systems was also evidenced by the UCA's navigation to servers hosting Company A software code and tools, specifically a code management and source code

repository hosting service named Bitbucket,⁶ shortly after gaining access to its network, as opposed to more generalized reconnaissance of Company A's network. More specifically, the UCA exfiltrated source code that is used, among other things, to unlock features on Company A communication devices that normally require additional payments for this software.

b. The EIS Team Observed the UCA's Use of a Comcast IP Address on September 28, 2020 and October 13, 2020

15. According to the EIS Logs, the UCA's changes to Individual B's account profile (namely the addition of UCA controlled phone numbers for two-factor authentication), occurred between 21:15:54 Universal Coordinated Time (UTC) and 21:30:26 UTC on September 28, 2020. According to the EIS Logs, the IP addresses associated with this activity were 18.216.71.43 and 73.159.4.46. According to an open source Whois query for IP addresses 18.216.71.43 and 73.149.4.46, these IP addresses resolved to Amazon Web Services ("AWS") and Comcast, respectively.

16. According to the EIS Logs, IP address 18.216.71.43 (the "AWS IP", or Subject Account 8)⁷ was identified as associated with UCA activity on September 28, 2020 during the period 21:15:54 UTC through 22:15:44 UTC. According to the EIS Logs, the IP address 73.149.4.46 ("Comcast IP") was identified as associated with

⁶ According to Bitbucket's parent company website, Bitbucket is a Git repository management solution designed for professional teams. Bitbucket gives users a central place to manage Git repositories, collaborate on source code, and guides users through the development process.

⁷ On December 30, 2020, the Honorable M. David Weisman, U.S. Magistrate Judge for the United States District Court for the Northern District of Illinois, issued a warrant to AWS for the search of Subject Account 8 and to Google for the search of an email account subscribed to "Andrew Mahn," namely andrewmahn@gmail.com ("Subject Account 7") (20 M 680 & 681).

UCA activity, specifically the activation of a new authentication factor for Individual B's Company A account, on September 28, 2020 at 21:30:26 UTC.

17. As detailed in the EIS Logs, the Comcast IP was associated with UCA activity again on October 13, 2020 from 17:26:55 UTC through 18:14:43 UTC; the hostname⁸ associated with this session was 'DESKTOP-J022HTC.' Notably, according to the EIS Logs, this hostname was first observed as associated with UCA activity on September 28, 2020, the first day of the cyber attack, at 22:31:46 UTC, or approximately one hour after the UCA first used the Comcast IP.

c. The Comcast IP Was Linked to MAHN's Logins to Company A's External Websites Prior to and During the Cyber Attack

18. According to Company A, an examination of Company A network logs revealed previous use of the Comcast IP to authenticate to Company A's externally hosted customer website during the period in which the UCA was sending spear-phishing emails to Company A employees and in the days preceding the EIS Team's mitigation of the cyber attack. The user credentials associated with these logins was "amahn@[Entity A].com."

19. According to Apple subscriber records for an Entity A cellular phone registered to MAHN, the email account amahn@[Entity A].com was used by MAHN. According to Company A, MAHN was formerly employed by Company A as a technician until approximately 2018, and was currently employed by Entity A. As part of his job at Entity A, MAHN purchased communications products from

⁸ According to techterms.com, and based on my training and experience, a hostname is a label that identifies a hardware device, or host, on a network. Hostnames can be modified by users, and the manner in which this is done varies based on a user's operating system software.

Company A on behalf of Entity A and regularly emailed with several Company A employees, including Individual B (one of the victims of the spear-phishing attack discussed above).

20. On or about November 9, 2020, Company A provided the FBI with email correspondence between MAHN and Company A employees. In these emails, MAHN communicated with Company A employees (using amahn@[Entity A].com) regarding part orders, license entitlements for Company A software products, and the programming of Company A devices.

21. According to Company A records, MAHN's Company A customer account, which required authentication via an identity management solution named Okta,⁹ was registered on or about August 16, 2019. According to Company A, anyone could create a Company A customer account. Creating such an account allowed users to view previous orders, manage previous orders, participate in blogs, and obtain information about Company A's products. According to Company A, in this respect, Company A's external website functioned much like an E-commerce website.

22. According to the EIS Logs, and supplementary computer network logs provided by the EIS Team ("Supplementary Logs"), MAHN used the Comcast IP to authenticate to Company A's external website and navigate to various Company A webpages, like 'business.[Company A].com', on August 16, August 17, August 22, August 24, August 26, August 28, August 31, September 2, September 3, September

⁹ According to its website, Okta is an identify management service solution that provides secure identity management with multi-factor authentication. Okta helps companies manage and secure authentication into applications.

16, October 14, October 15, and October 20, 2020—which is before and during the time period of the cyber attack.

23. According to logs for Company A's external website, MAHN used the Comcast IP in the days preceding the cyber attack and during the period of the cyber attack, which occurred during the period September 28, 2020 through approximately October 25, 2020. According to the EIS Logs, MAHN logged into Company A's external website (using his amahn@[Entity A].com account) with the Comcast IP on October 14, 2020 at 22:26:13 UTC, or approximately thirty hours after UCA activity was associated with the Comcast IP on October 13, 2020.

24. Notably, according to records from Google, approximately one day before on October 13, 2020 at 16:37:59 UTC, the UCA also logged into Subject Account 6 using the Comcast IP, or within approximately nineteen seconds of the UCA's observed activity on Company A's network. As discussed above, Subject Account 6 is the Google account associated with the Google Voice phone number used to socially engineer Individual B into giving up his Company A two-factor authentication code.

d. The User Agent Strings Associated with MAHN's Logins to Company A's Customer Website Match Those of the UCA During AWS Account Login

25. As detailed above, according to Company A, the UCA's first successful authentication to Company A's network using Individual B's stolen credentials occurred on September 28, 2020. According to the EIS Logs, the UCA's first activity on Company A's network utilized the AWS IP (Subject Account 8).

26. According to subscriber records from AWS, the AWS account had Account Number 878801018737, and was registered with apparently fictitious

information: the company name “commmot,” a Homer Glen, Illinois address that appears to be for a small network design company, Company A CEO’s first and last name, and email address “notification@comm-[Company A abbreviation].com.” According to NameCheap records, this subscriber information matched subscriber records for Subject Account 1, which is the NameCheap domain used to send spear-phishing emails to Company A employees beginning on August 7, 2020. (Notably, according to AWS Account subscriber records, Subject Account 8 was created on August 7, 2020.)

27. As detailed above, MAHN authenticated to Company A’s customer website using the Comcast IP in the period before and during the cyber attack. According to the EIS Logs and the Supplementary Logs, specifically the web application firewall logs, there were approximately twenty-eight instances during the period August 22, 2020 through November 26, 2020 in which the user agent string¹⁰ “Amazon CloudFront” was identified as the user agent string associated with (1) MAHN’s authentications and/or web traffic originating from the Comcast IP and (2) a second IP address used by MAHN, namely 65.96.153.157.

28. According to logs produced by AWS, the UCA logged into Subject Account 8’s user console on August 7, 2020 at 12:40:52 UTC using IP address 173.0.77.12. The following user agent string was associated with this login:

¹⁰ According to open sources, and based on my training and experience, a user agent string is an alphanumeric string that identifies the agent or program making a request to a web server for a resource, like a webpage or file. The user agent string contains the user application or software, the operating system and their versions, web client, web client version, and the engine responsible for the content display.

Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101
Firefox/79.0

29. According to the EIS Logs, approximately nine days later, on August 16, 2020 at 22:25:53 UTC, MAHN authenticated to Company A's external customer website using the Comcast IP. The following user agent string was associated with this login:

Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101
Firefox/79.0

30. As detailed above, the user agent string associated with the UCA's login to Subject Account 8 is an exact match for the user agent string associated with MAHN's logins to Company A's customer website on August 16, 2020.

31. Also according to the AWS Logs, the user agent string associated with the Subject Account 8 user console login on August 14, 2020 was as follows:

Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101
Firefox/79.0

32. As referenced above, according to the EIS Logs, this user agent string is an exact match for MAHN's authentication to the Chicago Company's customer website two days later on August 16, 2020. While a user agent string is not a unique identifier, based on my training and experience, identical user agent strings correlated with additional known identifiers can be used to characterize and attribute activity on a network to a specific cyber actor.

e. *The Comcast IP and other IP Addresses Used by the UCA During the Cyber Attack Were Used to Log into Subject Account 6*

33. As noted above, on October 30, 2020 the Honorable Jeffrey Cummings, U.S. Magistrate Judge for the U.S. District Court for the Northern District issued a

search warrant for Subject Account 6. According to records produced by Google in response, Subject Phone 1 (a Google Voice phone number) was associated with Subject Account 6. According to Google login records, the UCA logged into Subject Account 6 with nine unique IP addresses during the period August 8, 2020 through October 13, 2020. According to the EIS Logs and logs for Subject Account 8, most of these IP addresses were associated with UCA activity during the cyber attack.

34. For example, according to Google login records, the UCA logged into Subject Account 6 using IP address 194.99.105.76 on October 12, 2020. A query of the EIS Logs for this IP address revealed it was associated with UCA activity on Company A's network on October 12, 2020 between 10:55:55 UTC and 20:05:22 UTC. The hostname associated with this activity was DESKTOP-J022HTC. According to the EIS Logs, this hostname was also linked to UCA activity on October 13, 2020 at 17:26:55 UTC. Notably, the IP address associated with this activity was the Comcast IP.

35. Further, according to Google login records, the UCA logged into Subject Account 6 using the Comcast IP on October 13, 2020 at 16:37:59 UTC. According to the EIS Logs, the UCA used the Comcast IP to log into Company A's network on that date at 00:48:37 UTC.

f. Subject Account 6's search history Supports MAHN Being the UCA

36. The Google search warrant production for Subject Account 6 (the Google account linked to the Google Voice number involved in the spear-phishing campaign against Individual B) also included search history for Subject Account 6. The search

history identified both search terms used by the UCA and hyperlinks for sites visited by the UCA from Google searches.

37. A review of the search history revealed the UCA performed searches for information related to various stages of the cyber attack after logging into Subject Account 6. For example, according to the search history:

- On August 31, 2020, the UCA searched for "(224) 276-8645 Change Transfer Delete." Notably this is the phone number for Subject Phone 1 (the Google Voice number of Subject Account 6 that was used as part of the spear-phishing attack).
- On September 28, 2020 at 21:37:49 UTC, the day the UCA gained initial access to Company A's network using Individual B's stolen credentials, the UCA searched for "okta default method." (As discussed above, Okta provided two-factor authentication for Company A's network.)
- On October 2, 2020, the UCA searched for "bitbucket clone all" and visited a stackoverflow.com¹⁸ forum webpage titled "How to clone all git bitbucket repositories with a single script – Stack..." According to Company A, shortly after gaining initial access to Company A's network, the UCA navigated to a source code repository and code management solution employed by Company A named Bitbucket.
- On October 3, 2020, the UCA searched for "comm-[Company A abbreviation].com" (which is Subject Account 1, the website hosting the fake Company A login page used in the spear-phishing attack).

38. As detailed above, the aforementioned searches were consistent with information previously provided by Company A pertaining to the cyber attack. However, the search history also contained UCA search history that, based on MAHN's employment records, Company A external website navigation associated with MAHN's username amahn@[Entity A].com, and historical email correspondence between MAHN and Company A employees, appeared to identify MAHN as the operator of Subject Account 6. For example, according to the search history:

- On October 3, 2020 at 13:14:22 UTC, the UCA visited a website titled "ECAT online and/or Price options for [Company A device family ("Device Family 1")]-

Communications...” As part of the investigation, I viewed that webpage, which was a “communications.support” forum titled “ECAT online and/or Price options for [Device Family 1].” The first post in that thread referenced Device Family 1, model 7000.

- On October 7, 2020 at 23:40:49 UTC and 23:40:53 UTC, respectively the UCA searched for “cfx256” and visited another communications.support forum thread titled “CFX-256 encryption and Localized enable encryption.”

39. MAHN’s activity on Company A’s external website also included connections to the communications.support forum. More specifically, according to the EIS Logs, communications.support was identified as a unique referrer¹¹ associated with MAHN’s login credentials and the Comcast IP. The referrer URL appearing in the EIS Logs was [https://communications.support/threads/19125-5-year-warranty-breaks-\[Company A\]-FW-upgrade-policy?p\+127869](https://communications.support/threads/19125-5-year-warranty-breaks-[Company A]-FW-upgrade-policy?p\+127869) and was associated with a Company A customer account session beginning with MAHN’s authentication on September 2, 2020 at 16:31:51 UTC using the Comcast IP.

40. Additionally, a query of the EIS Logs for those events referencing Device Family 1 and associated with MAHN’s Company A customer account username amahn@[Entity A].com returned 136 GET¹² request events referencing Device Family 1. Further, the communications.support forum page named a specific model of Device Family 1, namely “7000.” According to email correspondence provided by Company A, on April 24, 2019, a Company A employee emailed MAHN at

¹¹ According to open sources, and based on my training and experience, referral traffic is akin to a recommendation from one website to another. Referral traffic is used to denote incoming traffic on a website as a result of clicking on a URL on another site.

¹² According to codeacademy.com, and based on my conversations with experienced FBI agents, a GET request is an HTTP request to a server to retrieve a specific resource, like a webpage it should display.

amahn@[Entity A].com. In her email to MAHN, with subject line “[Device Family 1] 7000,” Company A employee wrote:

Hello Andrew, The depo received the [devices] and repair line would like to find out what type of encryption keys should depot load back and return so the can be follow [sic] and proceeding accordingly. thank you.

41. On October 7, 2020, the UCA also performed a search for “(914) [redacted]-2023” and “914 area code.” According to Accurint Real Time Phone records and Company A employment records, that phone number was used by MAHN’s former manager at Company A.

42. Other searches in Subject Account 6 place the UCA in the same geographic area as MAHN and the **Subject Premises**. For example, according to the search history, on October 3, 2020 at 01:18:01 UTC, the UCA searched for “03301 weather.” According to the U.S. Postal Service’s website, 03301 is the zip code for Concord, New Hampshire. Additionally, on October 12, 2020 at 21:08:42 UTC and 21:08:46 UTC, the UCA searched for “boston weather.” According to Entity A’s website, Entity A is located in Boston, Massachusetts.

g. The UCA Interacted with Company A Systems of Which MAHN Had Direct Knowledge and Interacted with in His Position at Entity A

43. According to Company A, service depots were provided with Company A software tools (the “Depot Tools”) that enabled them to service Company A devices. Company A provided Depot Tools for every generation of Company A device. Company A’s control of Depot Tools was achieved through Flexera software licensing—namely, a Flexera license was needed to operate a Depot Tool. Further,

according to Company A, the Depot Tool was run on a host computer, which was connected to a device via a programming cable.

44. According to Company A, during the cyber attack, the UCA stole a Depot Tool used to unlock features on Company A devices that were manufactured in or prior to 2017. This limitation existed because the Depot Tool stolen by the UCA was only compatible with Company A firmware¹³ released prior to 2018. According to Company A, post-2017, licensing was handled via a newer web-based Depot Tool.

45. According to Company A records, the UCA logged into Company A's network on October 17, 2020 and, using stolen credentials, created a nine-year license for the aforementioned Depot Tool. According to Company A, this license allowed the UCA to unlock certain features on an unlimited number of Company A radios for nine years, or until 2029. Company A normally sells these software features at a price of up to \$175 per radio. Further, according to Company A, because firmware on Company A devices could be downgraded, the UCA could theoretically downgrade newly manufactured Company A devices to earlier firmware to unlock device features using the stolen Depot Tool.¹⁴

46. According to a Company A manager ("Individual D"), and based on prior email correspondence in which Individual D and MAHN were participants, MAHN

¹³ According to techterms.com, and based on my conversations with experienced FBI agents, firmware is a software program or set of instructions programmed on a hardware device.

¹⁴ Additionally, according to Individual D, also on October 17, 2020, the UCA accessed Company A's Flexera server and registered seven feature entitlements on a Company A radio with a known serial number. According to Company A, that radio was originally sold to a United Kingdom-based workforce communication and security solution company. However, according to Individual D, subsequent resales or transfers of radios would not necessarily be noted in Company A records.

was responsible for radio management and would be familiar with how Company A licenses its Depot Tools. Based on that correspondence, it appeared MAHN had specific knowledge regarding Device Family 1 licensing. According to Individual D, in Company A email correspondence involving Individual D and MAHN, using amahn@[Entity A].com, MAHN inquired about past-due licensing and capacity licenses relating to a device management software used to manage Device Family 1. According to Individual D, Individual D was included in email correspondence dated September 7, 2019 to MAHN, using amahn@[Entity A].com, in which Entity A was emailed Device Family 1 licenses that it purchased from Company A. These licenses permitted Entity A to expand its Device Family 1 radio management by 2,000 additional devices.

47. Additionally, according to Company A, in 2017 a Company A employee ("Individual C") received an email from MAHN's former Company A manager requesting access to a web-hosted Depot Tool that eventually supplanted the Depot Tool stolen by the UCA. MAHN's former manager requested this access for MAHN. Individual C assessed MAHN likely had familiarity with Company A Depot Tools based on his granted access to the new web-based Depot Tool in 2017 while still employed by Company A.

48. As detailed above, MAHN engaged in regular email correspondence with multiple Company A employees. This correspondence included Individual B and others targeted by the UCA during the spear-phishing campaign. According to emails from Company A, MAHN, using amahn@[Entity A].com, received or was carbon-

copied on emails in which Company A sent licensing information or entitlement IDs for specific Company A products.

h. *The Comcast IP Connects MAHN to the Cyber Intrusion*

49. According to subscriber records provided by Comcast, the Comcast IP was assigned to a customer named ‘Susan Hart’ during the period August 13, 2020 through August 23, 2020 and was registered with the email address mycircuits@protonmail.com.¹⁵ As detailed above, MAHN used the Comcast IP to authenticate to Company A’s customer website using the credentials amahn@[Entity A].com beginning on August 16, 2020, or during “Susan Hart’s” lease term. Also according to Comcast subscriber records, “Susan Hart” was assigned another IP address (73.4.28.180) from August 13, 2020 at 23:49:49 UTC through August 15, 2020 at 19:30:00 UTC.

50. Additionally, at least two of MAHN’s personal accounts were accessed using the second “Susan Hart” IP address (73.4.28.180). According to transaction records provided by Venmo for MAHN’s Venmo account registered with Subject Account 7 (andrewmahn@gmail.com), MAHN initiated two transfers to his Venmo-linked bank account on August 9, 2020 using IP address 73.4.28.180. Similarly, according to Google records for Subject Account 7 (andrewmahn@gmail.com), MAHN also logged in using IP address 73.4.28.180 on August 9, 2020 at 21:42:29 UTC.

¹⁵ According to NameCheap records, Subject Account 1 (the domain used to create the email account used to spear-phish Company A employees, or Subject Account 4), was registered with mycircuits@protonmail.com, which matched the registration email used to register “Susan Hart’s” account.

51. According to Comcast subscriber records, the service address for Susan Hart's Comcast account was listed as ¹⁶

According to Accurint records, Susan Hart was associated with an address in Winthrop, Massachusetts. However, public and government records available via Accurint, and a query of Massachusetts records conducted by the FBI's Boston, Massachusetts office on or about November 3, 2020, returned no other records for an individual named Susan Hart residing at that address.

52. According to a Comcast employee, Comcast was unable to locate a lessee of the Comcast IP during the period August 23, 2020 through October 28, 2020 despite MAHN's use of the Comcast IP in August, September, and October 2020 to log in to Subject Account 7. According to Comcast's Xfinity website, an individual can obtain Comcast Internet service and verify a Comcast account via an online registration process. Therefore, it appears that MAHN used a fictitious person ("Susan Hart") to register internet service in an attempt to anonymize his online activity.

i. Funds Used to Pay for the UCA NameCheap Spearphishing Account Originated from MAHN

53. As detailed above, the UCA created a NameCheap account on August 6, 2020 at 19:08:36 UTC which hosted the domain comm-[Company A abbreviation].com and multiple email addresses (Subject Account 2, Subject Account 3, and Subject Account 4) used to spear-phish Company A employees and exfiltrate credentials from

¹⁶As detailed above, according to Accurint records and emails from the electricity and natural gas provider National Grid sent to Subject Account 7, MAHN resided on Edgehill Road in Winthrop, MA (the "Winthrop Address") during the time period of the UCA spear-phishing campaign and cyber attack.

Company A's network.¹⁷ According to NameCheap records, on August 6, 2020 at 23:18:20 UTC, NameCheap recorded a transaction notated as "DEPOSIT BITPAY" with transaction number FM9HZ132V6iBd327eX6LGn in the amount of \$26.15. According to Bitpay¹⁸ records, the transaction date and time associated with this transaction number was August 6, 2020 at 23:18:18 UTC. The merchant identified was "Namecheap.com."

54. According to Google search history records for Subject Account 7 (andrewmahn@gmail.com), MAHN performed a search for "blockchain" on August 6, 2020 at 23:12:47 UTC, and then visited Blockchain.com approximately two seconds later. This search occurred approximately six minutes before the UCA—now believed to be MAHN—paid for the NameCheap account used to conduct the spearphishing attack on Company A.

55. Relatedly, according to Google email records for Subject Account 7 (andrewmahn@gmail.com), MAHN received an email at Subject Account 7 from Blockchain.com, email address notify@wallet-tx.blockchain.com, with subject line "Authorize log-in attempt." The email contained the following message:

Authorize Log In Attempt

An attempt to login to your Blockchain wallet was made from an unknown browser.
Please confirm the following details are correct:

¹⁷ According to the EIS Report, after gaining access to a Company A server, the UCA changed its configuration to collect and then email user credentials and passcodes to sds@comm-[Company A abbreviation].com. A review of search warrant production for the Namecheap account revealed tens of examples of the UCA receiving emails from sds@[Company A].com (Subject Account 3), with x-mailer "ColdFusion 9 Application Server," containing the username and passwords of Company A employees with access to that server.

¹⁸ According to finance.yahoo.com, Bitpay is a Bitcoin payment service provider based in Atlanta, Georgia. Bitpay is the largest Bitcoin payment processor in the world, and enables businesses to accept payments in Bitcoin and Bitcoin Cash and send those funds directly to a bank account.

Time: 2020-08-06 23:15:31 GMT [UTC]
 Browser: Firefox 7
 Operating System: Windows 10.

56. As highlighted by the above email, MAHN logged into his Blockchain wallet approximately three minutes before the UCA made a payment to NameCheap at 23:18:18 UTC. Additionally, as detailed above, the operating system associated with the above-referenced login to Blockchain.com matches the operating system used by the UCA to log into Subject Account 8 (AWS IP) and the operating system associated with MAHN's authentications to Company A's customer website.

57. The funds that paid for the NameCheap account used in the spear-phishing attack on Company A can be identified as originating from MAHN's account at a virtual currency exchange named Coinbase ("Coinbase Account"). Specifically, according to Coinbase records, on or about December 21, 2017,¹⁹ MAHN initiated a transfer of .01 Bitcoin²⁰ (BTC) from the Coinbase Account, registered with Subject Account 7 (andrewmahn@gmail.com)²¹, to BTC address²²

¹⁹ According to Chainalysis records, which are recorded in UTC, this transaction was published to the blockchain in the morning hours of December 22, 2017.

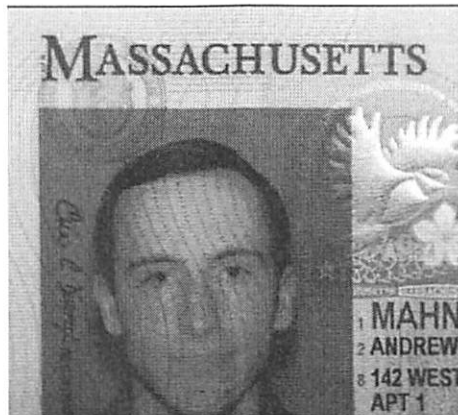
²⁰ Based on my training and experience, I know that BTC is a decentralized virtual currency, which is circulated over the Internet, but which is not backed by a government. BTC is supported by a peer-to-peer network. All transactions are recorded on BTC's public ledger, called the 'blockchain.' Although transactions are visible on the public ledger, each transaction is only listed by a complex series of number that does not identify the individuals involved in the transaction.

²¹ MAHN's association with the Coinbase Account was identified during a review of emails contained in Subject Account 7. Specifically, on June 2, 2018, MAHN received an email from 'Coinbase' no-reply@coinbase.com at Subject Account 7 with subject line "A deposit for \$50.00 USD has been started." The following message appeared in the body of same email: "Hi Andrew, On Saturday Jun 2, 2018 you authorized Coinbase to fund your Stored Value Account with \$50.00 from your linked bank account. We have debited your linked bank account accordingly."

²² Based on my training and experience, I know that—like sending and receiving an email via an email address, a user can send and receive BTC via a BTC address.

1GWVU3vdT4rG8XjNeYcRSVaAc4F1EmwWms ("BTC Address 1"). According to Coinbase records, the two-factor authentication code for this transaction was sent to the phone number 321-829-4141. According to Google subscriber records, 321-829-4141 is a Google Voice number registered to Subject Account 7 (andrewmahn@gmail.com).

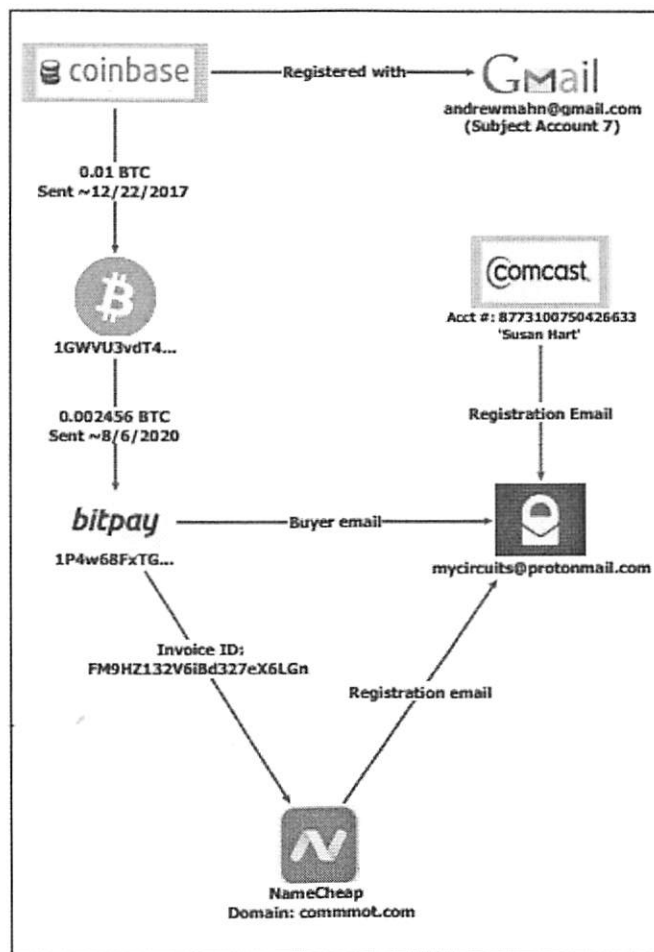
58. Based on my training and experience, US-based exchanges require customers to verify their identities during account registration in an effort to combat money laundering. In this case, according to Coinbase records, MAHN submitted a photo of himself as well as his Massachusetts driver's license during Coinbase Account creation, as excerpted below:





59. According to open source analysis of blockchain transactions associated with BTC Address 1 analysis, the only deposit to BTC Address 1 was from MAHN's Coinbase account for 0.01 BTC on December 22, 2017. Also according to blockchain analysis, the 0.01 BTC remained unused in BTC Address 1 until August 6, 2020, when .002456 BTC was transferred to a Bitpay address, namely 1P4w68FxTGFB5NZQ9Cbb6wR4yAgGFF7iVr ("BTC Address 2"). According to Bitpay records, the invoice ID associated with BTC Address 2 on that date, FM9HZ132V6iBd327eX6LGn, was intended for the benefit of NameCheap and the buyer's email was listed as mycircuits@protonmail.com.

60. As detailed above, mycircuits@protonmail.com was used to register the UCA NameCheap account and the Susan Hart Comcast account. A link chart representation of the aforementioned virtual currency transactions, as well as MAHN's connection to facilities associated with these transactions, appears below:



j. *MAHN Purchased and Received Equipment at the His Prior Residence Likely Employed to Create the Susan Hart Comcast Account*

61. Based on my review of emails received by MAHN using Subject Account 7 in the days preceding the first observed days of UCA activity, my training and experience, and information provided by other experienced FBI agents, MAHN appears to have researched the provisioning of a second IP address at the Winthrop Address and ordered the networking equipment necessary to create the Susan Hart account using a preexisting Comcast connection.

62. More specifically, according to Google search history records for Subject Account 7 (andrewmahn@gmail.com), on July 25, 2020 and July 27, 2020, MAHN performed the following searches:

- “comcast second wan port” on July 25, 2020 at 15:10:40 UTC
- “comcast additional ip” on July 25, 2020 at 15:11:15 UTC
- “comcast second wan port” on July 25, 2020 at 15:21:29 UTC
- “comcast second ip” on July 27, 2020 at 19:22:42 UTC
- “second ip xfinity” on July 27, 2020 at 19:24:13 UTC
- “comcast business account” on July 27, 2020 at 19:25:43 UTC

63. According to Subject Account 7 emails dated August 2, 2020 through August 4, 2020 from ebay@ebay.com, MAHN ordered the following Internet networking equipment to be delivered to the Winthrop Address:

- Arris SB6190 DOCSIS 3.0 Cable modem;
- 2 Way Digital 1Ghz High Performance Coax Cable Splitter; and
- Motorola Signal Booster Broadband Drop Amplifier

64. As detailed above, the use of the Comcast IP by the UCA during the cyber attack was only captured by Company A’s network logs on two occasions (in September and October 2020) during the cyber attack, indicating the separate Comcast account was created to provide an additional layer of obfuscation beyond the use of VPN services like ProtonVPN and the above-referenced UCA infrastructure registered with fake information.

i. Subject Account 7 search history Supports MAHN Being the UCA

65. As detailed above, the UCA stole a depot tool during the cyber attack used to unlock features on Company A radios. According to Individual D, a Flexera-developed software license manager was used to manually license the Depot Tool stolen by the UCA during the cyber attack. According to Individual D, on October 17,

2020, the UCA accessed Company A's Flexera server and registered seven entitlements on a radio with a known serial number after licensing the Depot Tool for nine years.

66. According to Google search history for Subject Account 7 (andrewmahn@gmail.com), MAHN performed multiple searches using search terms that referenced Flexera, Flexera-related tools, or Company A entitlements registered using Flexera beginning on October 16, 2020—which was just one day prior to the UCA's use of Flexera to register entitlements on a Company A device. A subset of these searches follows:

- On October 16, 2020 at 19:07:12 UTC, MAHN searched for “flexnet operations”;
- On October 16, 2020 at 19:07:59 UTC, MAHN searched for “flexera trial”;
- On October 16, 2020 at 19:15:02 UTC, MAHN searched for “FlexNetOperations_2020-R1_installer.bin”;
- On October 16, 2020 at 19:57:10 UTC, MAHN searched for “flexnet makekey”;
- On October 16, 2020 at 19:57:34 UTC, MAHN searched for “FLEXIm Programmers Guide”;
- On October 16, 2020 at 20:01:16 UTC, MAHN searched for “Imcrypt manual”;
- On October 16, 2020 at 20:06:13 UTC, MAHN searched for “flexnet eid [Entitlement IDs]”;
- On October 17, 2020 at 23:27:07 UTC, MAHN searched for “[Company A] cap max eid”;
- On October 17, 2020 at 23:27:11 UTC, MAHN visited “[Company A] EID Reference Charts | North Georgia Communications”;
- On November 14, 2020 at 15:08:31 UTC, MAHN searched for “HLKN4463”;
- On November 14, 2020 at 15:08:58 UTC, MAHN searched for “Canada full frequency range eid”; and
- On November 15, 2020 at 14:44:20 UTC, MAHN searched for “flexera license.dat.”

67. As referenced above, MAHN's Flexera-related searches can be correlated with the UCA's activity recorded in the EIS Logs. Additionally, one of the searches listed above can also be correlated with searches appearing in the search

history for Subject Account 6 (the UCA Google account associated with Subject Phone 1). Specifically, according to Google search history for Subject Account 6, on October 13, 2020 at 17:24:59 UTC and 17:34:06 UTC, the UCA visited a website titled ‘Imcrypt security – Community – Flexera Community and a website titled “HOW TO build your own Imcrypt – Wire Free Alliance,’ respectively. On November 20, 2020, I navigated to one of the websites referenced above, namely ‘Imcrypt security – Community – Flexera Community,’ which resolved to a Reverera²³ Community forum regarding the topic of “Imcrypt Security” and employees using imcrypt to create unauthorized licenses.

68. Lastly, as detailed above, according to Individual D, on October 17, 2020, the UCA accessed Company A’s FlexNet server and registered seven entitlements on a radio with a known serial number. On January 28, 2020, I viewed the website visited by MAHN titled “[Company A] EID Reference Charts | North Georgia Communications.” This webpage contained a list of entitlements, or Company A features, that could be unlocked on Company A communication devices.

j. MAHN Searched for a Company A Employee’s Name Six Minutes Before That Employee Received a Spear-Phishing Email from Subject Account 4

69. As detailed in the Supplementary Logs, multiple Company A employees began receiving spear-phishing emails from the UCA on August 7, 2020. More specifically, on August 7, 2020 at 01:20:25 UTC, no-reply@comm-[Company A abbreviation].com (Subject Account 4) sent the first known spearphishing email to a Company A employee (“Individual F”) at his Company A email address.

²³ According to Reverera’s website, Flexera’s Supplier Division is now named “Reverera.”

70. According to Google search history for Subject Account 7 (andrewmahn@gmail.com), on August 7, 2020 at 01:14:51 UTC MAHN performed a search for “[Individual F] [Company A].” Notably, MAHN performed this search *just six minutes* before the UCA sent a spear-phishing email to Individual F’s Company A email address.

k. MAHN Searched for a Company A’s Source Code Repository During the Spear-Phishing Campaign and After the Cyber Attack

71. As detailed above, according to the EIS Logs, after gaining access to Company A’s network on September 28, 2020, the UCA navigated to a Company A source code repository and code management solution named Bitbucket. According to Company A, the UCA’s immediate navigation to Bitbucket, as opposed to engaging in general reconnaissance and network enumeration, was indicative of the UCA’s familiarity with Company A’s network.

72. According to Google search history for Subject Account 7 (andrewmahn@gmail.com), MAHN performed searches for Bitbucket and visited its website on August 30, 2020 and November 9, 2020. Specifically, on August 30, 2020, MAHN searched for “bitbucket” at 16:31:35 UTC and visited a Bitbucket webpage, <https://bitbucket.org/product> at 16:31:39 UTC. According to the Supplementary Logs, as of August 30, 2020 the UCA was already engaged in a spear-phishing campaign against Company A employees and was attempting to authenticate to Company A’s network using stolen credentials.

73. Also according to Google search history for Subject Account 7, on November 9, 2020, MAHN searched for “bitbucket” at 12:17:59 UTC. Notably,

according to those records, immediately prior to searching for "bitbucket," MAHN performed a search for "[Company A Device Family 2] system key" at 12:14:29 UTC. According to Company A, the UCA exfiltrated source code related to Device Family 2 in addition to the Depot Tool.

l. MAHN's Subject Account 7 Searches in the Days Preceding the Spear-Phishing Campaign Reveal an Interest in Hacking, Radio Service Software, and UCA Infrastructure

74. As detailed above, the UCA's spear-phishing campaign against Company A Employees began on August 7, 2020. As also detailed above, in the days immediately preceding the receipt of spear-phishing emails by Company A employees, MAHN conducted research regarding the acquisition of an additional Comcast IP address and purchased equipment that could be used to register an additional Comcast account at his residence.

75. However, approximately one month before MAHN appeared to take affirmative steps towards the procurement of infrastructure used in the cyber attack, MAHN performed multiple searches that appear to show an interest in hacking, data to be exfiltrated, and targets of a prospective hack. Some examples of these searches from Subject Account 7 (andrewmahn@gmail.com) are excerpted below:

- 07/11/2020, 20:48:04 UTC - searched for "must watch hacker movies"
- 07/11/2020, 20:48:10 UTC - visited 'The Complete List of Hacker and Cybersecurity Movies'
- 07/11/2020, 20:51:37 UTC - searched for "must see hacker movies"
- 07/13/2020, 17:42:10 UTC - searched for "namecheap promo code"
- 07/20/2020, 17:31:21 UTC - searched for "radiosoftware [Company A] icom"
- 07/20/2020, 20:06:39 UTC - searched for "Radio service software - HackersRussia"
- 07/21/2020, 00:01:41 UTC - visited 'Index of /radiosoftware/[Company A]/ - RSWS'

- 07/21/2020, 00:08:52 UTC - visited 'Публикации [Company A] - Клуб любителей радиостанций [Company A],' which machine translated to 'Publications [Company A] – [Company A] Radio Club'
- 07/21/2020, 00:11:19 UTC - visited 'HACKERSRUSSIA'S PUBLIC FTP'
- 07/21/2020, 00:12:10 UTC - visited 'RADIOSOFTWARE RU: radio software download'
- 07/24/2020, 20:06:40 UTC - searched for "myview.[Company A].com"

76. Notably, MAHN also searched for NameCheap (the domain provider used by the UCA to spear-phish Company A employees and exfiltrate credentials from Company A's network), and Company A's radio service software. As detailed above, during the cyber attack the UCA exfiltrated Depot Tool software that could be used to unlock features on Company A radios.

m. MAHN Currently Resides at the Subject Premises

i. MAHN Purchased the Subject Premises on January 28, 2021

77. As described above, MAHN received equipment likely used to create the 'Susan Hart' Comcast account at the Winthrop address. However, according to records for MAHN's Wings bank account, it appeared MAHN purchased the **Subject Premises**, located at 15 Craven Terrace, Derry, New Hampshire, on January 28, 2021.

78. Specifically, according to Wings bank account records for an account owned by "Andrew Mahn" address PO Box 266 Hudson NH 03051 US²⁴, on December 28, 2020, MAHN wrote a check for Keller Williams Coastal Realty in the amount of \$5,000.00. Appearing in the note section of the check was the handwritten text "15 Craven Ter. Derry." According to Google search history records for Subject Account

²⁴ As detailed above, this address was listed on MAHN's Subject Account 9 invoice.

7, MAHN performed a search for “15 craven derry gis” on December 27, 2020 at 13:23:52 UTC, “15 Craven Ter. Derry, NH 03038” (which is the address of the **Subject Premises**) on December 26, 2020 at 20:47:14 UTC, and visited “15 Craven Ter, Derry, NH, 03038 | realtor.com” on December 23, 2020 at 15:49:22 UTC.

79. According to a Zillow.com listing²⁵ for the **Subject Premises**, the **Subject Premises** was pending sale on December 28, 2020, which matches the date of the above-referenced check. The Zillow listing identified the source of this information as “Keller Williams via MLS.” Further, according to the Zillow listing, the **Subject Premises** was sold on January 28, 2021.

80. Based on my training and experience, it appears the \$5,000 check to Keller Williams Coastal Realty was an earnest money check for the purchase of the **Subject Premises**.

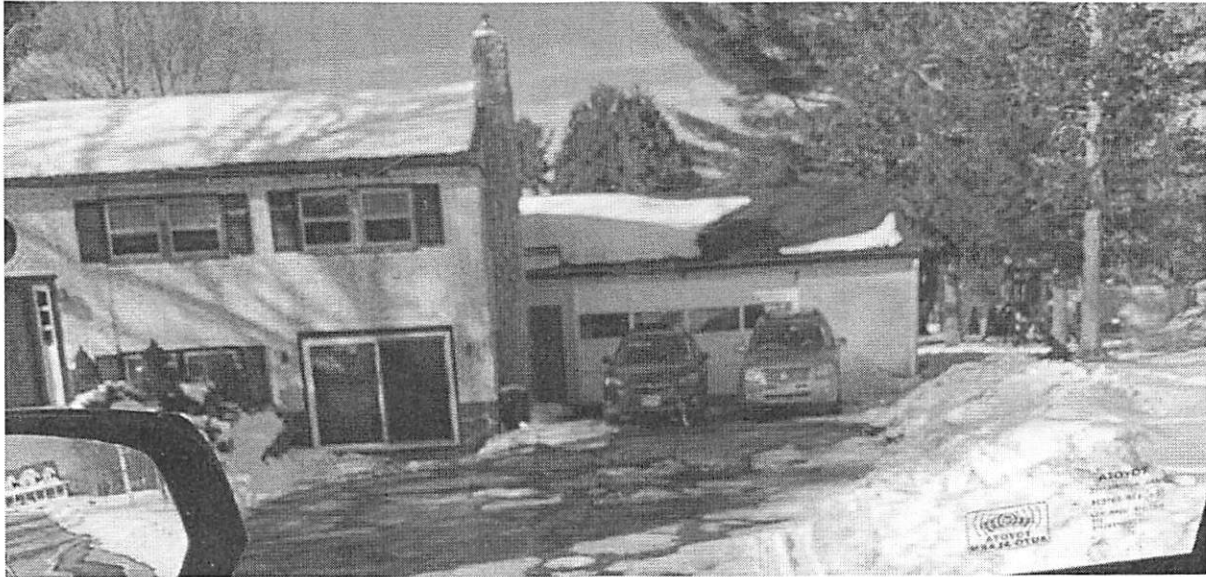
ii. FBI Surveillance of MAHN Conducted Between February 13, 2021 and February 24, 2021 Confirms MAHN Currently Resides at the Subject Premises

81. According to New Hampshire vehicle registration records, a gray Subaru Crosstrek, License Plate Number 4480940, was registered to MAHN.

82. On February 13, 2020, FBI Boston Field Office initiated surveillance of the **Subject Premises**. On the same date at approximately 14:30 Eastern Standard Time (“EST”) an FBI Special Agent observed a gray Subaru Crosstrek and a blue Mercury Mariner at the **Subject Premises**. A photo taken by the FBI Special Agent

²⁵ Accessed on February 23, 2021 and available at https://www.zillow.com/homedetails/15-Craven-Ter-Derry-NH-03038/86807428_zpid/.

on February 13, 2020 of said vehicles parked in the driveway of the **Subject Premises** appears below:



83. On February 25, 2021, two FBI Special Agents initiated surveillance of the Subject Premises at 03:50 EST. On same date at 05:02 EST, a Subaru Crosstrek, “dark in color” bearing New Hampshire license plate number 4480940 was observed leaving the **Subject Premises** and following a direct route to a nearby on-ramp for I-93 South.

84. According to Google Maps, the most direct route from the **Subject Premises** to Entity A’s address is I-93 South.

n. Computing, Mobile, and External Storage Devices Are Likely to Contain Evidence of the Subject Offenses

85. As detailed above, MAHN maintained a virtual currency account²⁶ used to pay for UCA infrastructure. According to Investopedia.com, a virtual currency

²⁶ According to Investopedia.com, and based on my training and experience, a virtual currency wallet is analogous to a physical wallet. However, instead of storing physical

wallet is a software program into which virtual currency is stored. Virtual currency wallets come in many forms, the four main types of which are desktop, mobile, web, and hardware.

86. According to play.google.com and apps.apple.com, Blockchain.com has a mobile cryptocurrency wallet application for android and iOS with tens of millions of users worldwide. The mobile application permits users to buy, sell, hold, send, receive, and earn interest in the wallet brokerage.

87. According to play.google.com and apps.apple.com, Coinbase has a mobile application for android and iOS permitting users access to the world's largest cryptocurrency exchange. According to blog.coinbase.com, Coinbase also allows users to view their wallet transaction history.

88. According to play.google.com, Keepass has a mobile application named 'Keepass2Android Password Safe.' According to the application's description, Keepass2Android is compatible with KeePass Password Safe v1 and v2 for Windows and aims at simple synchronization between devices. According to an August 19, 2020 email from tracking@shipstation.com to Subject Account 7, MAHN received delivery of an android device, namely a Samsung Galaxy S10e smartphone, on same date. Notably, according to Google Device List records for Subject Account 7, the only mobile devices used to access Subject Account 7 since June 9, 2020 were two iPhones—however, MAHN received delivery of the Samsung Galaxy approximately twelve days after the UCA began the spear-phishing campaign against MSI

currency, the wallet stores relevant information such as secure private keys used to access public virtual currency addresses and carry out transactions.

employees, indicating that the Samsung Galaxy device may have been employed as another form of UCA infrastructure.²⁷

89. As highlighted above, MAHN received multi-factor authentication messages and notifications when accessing multiple services, some of which link MAHN to infrastructure or IP addresses utilized by the UCA during the cyber attack. Also based on my training and experience in cyber-related investigations, cyber actors utilize mobile devices and hardware tokens to access operational infrastructure and personal accounts containing evidence of the **Subject Offenses**. In the specific example referenced immediately above, MAHN appeared to use a mobile device to socially engineer Individual B into providing his Okta two factor authentication code. Further, as described by Coinbase's website, a virtual currency transaction history may be available via a search of MAHN's mobile devices. Lastly, based on my training and experience in computer-related investigations, a search of contact lists and other data stored directly on mobile device hardware frequently leads to the identification of additional facilities used by cyber actors in furtherance of the **Subject Offenses** and co-conspirators.

o. Training and Experience

90. Based on my training and experience in computer-related investigations, I believe that a search of the **Subject Premises** will likely yield the following types of evidence relating to the **Subject Offenses**:

²⁷ According to the EIS Report, Individual B began receiving social engineering SMS text messages as early as August 31, 2020.

- a. the identity of the individual (and any potential co-conspirators) involved in the spear-phishing and cyber attack against Company A;
- b. the identification of additional communication accounts utilized by the UCA;
- c. the methods, techniques, and tools used to conduct the illegal activities;
- d. device(s) used to store stolen data from Company A during the cyber attack;
- e. device(s) employing stolen code or tools stolen from Company A during the cyber attack;
- f. item(s) and/or document(s) related to the shipment of Company A devices employing stolen Company A code or software;
- g. proceeds related to the shipment of Company A devices employing stolen Company A code or software; and
- h. item(s) or device(s) used to store virtual currency wallet(s) used to pay for attacker infrastructure.

III. SEARCH PROCEDURE

91. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (*e.g.* computer hardware, computer software, computer-related documentation, and cellular telephones) to be processed later by a

qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an electronic storage media system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

c. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any

applications software which may have been used to create the data (whether stored on hard disk drives or on external media).

d. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s) and are subject to seizure as such if they contain contraband or were used to carry out criminal activity.

92. When searching the **Subject Premises**, it is likely that Apple brand devices, such as iPhones or iPads, will be found (as discussed above). I know from my training and experience and my review of publicly available materials published by Apple that those Apple devices can enable what is referred to as "Touch ID," a feature that recognizes up to five fingerprints designated by the authorized user of the iPhone. A Touch ID sensor, a round button on the iPhone or iPad, can recognize fingerprints. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require.

93. The Touch ID feature only permits up to five attempts with a fingerprint before the device will require the user to enter a passcode. Furthermore, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device

based on a fingerprint alone. Similarly, Touch ID will not allow access if the device has been turned on or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful.

94. For these reasons, it is necessary to use the fingerprints and thumbprints of any device's users to attempt to gain access to any Apple devices found at the **Subject Premises** while executing the search warrant. The government may not be able to obtain the contents of the Apple devices if those fingerprints are not used to access the Apple devices by depressing them against the Touch ID button. Although I do not know which of the ten finger or fingers are authorized to access on any given Apple device and only five attempts are permitted, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for Touch ID, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

95. I also know from my training and experience and my review of publicly available materials published by Apple that those Apple devices can enable what is referred to as 'Face ID.' According to Apple's website, upon completing Face ID setup, which involves enrolling a user's face, users can securely unlock their iPhone or iPad by glancing at the device's screen rather than entering a passcode. Face ID allows permits users to authorize purchases and sign into applications. The government may not be able to obtain the contents of the Apple devices if it is not unlocked using the aforementioned Face ID facial recognition secure unlock feature.

96. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

97. The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

IV. CONCLUSION

98. Based on the above information, I respectfully submit that there is probable cause to believe that evidence, instrumentalities, and fruits of violations of Title 18, United States Code, Sections 1030 and 1343 are located at the **Subject Premises**, further described in Attachment A. By this affidavit and application, I request that the Court issue a search warrant for the **Subject Premises**, authorizing the seizure of the items described in Attachment B, pursuant to the protocol described in the addendum to Attachment B.

FURTHER AFFIANT SAYETH NOT.

/s/ Damien A. Colon

Damien A. Colon
Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference this 17th day of March, 2021, pursuant to Fed. R. Crim. P. 4.1, and affirmed under oath the content of this affidavit and application.

Andrea K. Johnstone

HON. ANDREA K. JOHNSTONE
United States Magistrate Judge



ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The **Subject Premises** is the single family house located at 15 Craven Terrace, Derry, New Hampshire. The house is a white, two-story residence with a red front door and an attached two-car garage. The number "15" is written on the mailbox post in front of the house. The **Subject Premises** is pictured below:



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Evidence, instrumentalities, contraband, and fruits concerning violation of Title 18, United States Code, Sections 1030 and 1343 (the “**Subject Offenses**”), as follows:

1. Documents and objects concerning occupancy, ownership, or control of the **Subject Premises**.
2. Items related to computer intrusions, including spearphishing.
3. Items related to Company A.
4. Company A source code.
5. Items related to Company A passwords, login information, document downloading, or any unauthorized computer access.
6. Items relating to the sale of Company A products, features, source code, including unlocking of features on Company A devices.
7. Items related to NameCheap or AWS accounts used in the **Subject Offenses**.
8. Items relating to BitPay, Coinbase or other cryptocurrency accounts used in the **Subject Offenses**.
9. Items related to the identities and contact information of participants in or witnesses to the **Subject Offenses**.
10. Items related to the state of mind of participants in the **Subject Offenses** at or near the time of the **Subject Offenses**.

11. Any passwords, encryption keys, security keys, code generators, or other devices that may be necessary to access any electronic equipment or accounts.

12. Electronically-stored data consisting of the items to be seized set forth in Attachment B.

13. Information which tends to identify the user(s) of or person(s) with control over or access to any electronic storage media in which any of the items described in Attachment B are found.

14. During the execution of this search warrant at the **Subject Premises**, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of persons at the **Subject Premises** onto the Touch ID sensor of any Apple iPhone, iPad, or other Apple brand device in order to gain access to the contents of any such device.

ADDENDUM TO ATTACHMENT B

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B; and
- d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.